21-MJ-6528 -MPK
21-MJ-6529-MPK
21-MJ-6530-MPK

AFFIDAVIT OF SPECIAL AGENT JACQLEEN CUNNINGHAM IN SUPPORT OF APPLICATIONS FOR TWO CRIMINAL COMPLAINTS AND A SEARCHWARRANT

I, Jacqleen Cunningham, being duly sworn, hereby depose and state as follows:

Agent Background

1. I am a Special Agent with Homeland Security Investigations ("HSI") and have been so employed since June 2010. I have successfully completed a training program in conducting criminal investigations at the Federal Law Enforcement Training Center in Brunswick, Georgia. In 2007, I graduated from Sacred Heart University with a Bachelor of Science Degree in Criminal Justice. My current assignment as an HSI Special Agent includes conducting and participating in investigations involving the fraudulent acquisition, production, and misuse of United States immigration documents, United States passports, and various identity documents. Due to my training and experience, as well as conversations with other law enforcement officers, I am familiar with the methods, routines, and practices of document counterfeiters, vendors, and persons who fraudulently obtain or assume false identities.

2. I am also a member of HSI's Document and Benefit Fraud Task Force ("DBFTF"), a specialized field investigative group comprised of personnel from various local, state, and federal agencies with expertise in detecting, deterring, and disrupting organizations and individuals involved in various types of document, identity, and benefit fraud schemes. The DBFTF is currently investigating a group of suspects who are believed to have obtained stolen personally identifiable information ("PII") of other United States citizens from Puerto Rico and elsewhere. Many of these individuals used the stolen identities to open bank accounts and/or

credit cards to fraudulently purchase, register, and/or export vehicles as part of a multi-state scheme involving financial fraud, auto theft, and the exportation of stolen goods. Subsequent investigation has established that this group also has successfully used some victims' PII to apply for United States Small Business Administration ("SBA") Economic Injury Disaster Loans ("EIDLs").

3. I am submitting this affidavit in support of criminal complaints charging (1) Edwin ACEVEDO ("ACEVEDO"), date of birth xx-xx-1985, with conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349 (the "Target Offense") and (2) [redacted].

4. I also submit this affidavit in support of an application for a search warrant for the following property: [redacted] Trillium Circle, Acton, Massachusetts ("Target Location"), as described more fully in Attachment A. I have probable cause to believe that this property contains evidence, fruits, and instrumentalities of the Target Offense, as described in Attachment B.

5. The facts in this affidavit come from my personal involvement in this investigation, including interviews of witnesses, and my review of documents and bank records, as well as my conversations with other members of law enforcement. In submitting this affidavit, I have not included every fact known to me about this investigation. Instead, I have only included facts that I believe are sufficient to establish probable cause.

Background of Investigation

6. Since approximately January 2019, HSI special agents have been investigating a scheme involving the use of stolen identities to fraudulently open bank accounts, obtain credit

cards, and purchase vehicles, many of which are then exported out of the United States. More specifically, the investigation has revealed a number of individuals using the stolen identities of United States citizens from Puerto Rico to fraudulently finance late-model vehicles from dealerships in Massachusetts, paying zero dollars down. At the dealerships, the individuals provide a variety of fraudulent identification and credit-related documents, including fraudulent Puerto Rico driver's licenses and social security cards as proof of identification. The perpetrators of this fraudulent scheme typically do not make payments on the vehicles, resulting in the dealership or relevant lending financial institution taking a total loss for the vehicles. The individuals have also been successful in opening bank accounts in the same stolen identities prior to fraudulently purchasing the vehicles. Individuals perpetrating the scheme max out associated credit cards within days or weeks and rarely make any payments on the accounts. More recent investigation has also revealed that some of these same individuals, including Alvin RIVERA – along with Joseph CRUZ, Darwyn JOSEPH, Neida LOPEZ, ACEVEDO and [redacted] – were also involved in a scheme to use stolen identities to open bank accounts, to apply for EIDLs from the SBA and elsewhere, to accept funds from those loans through transfers into the fraudulent bank accounts, and to launder the funds.

Probable Cause

Background of Investigation; Identification of ACEVEDO and [redacted] as Co-Conspirators with RIVERA and Others

7. On or about September 9, 2020, HSI Special Agent Timothy Taber, with whom I am working on this investigation, submitted to this court an affidavit in support of a criminal complaint charging Alvin RIVERA ("RIVERA") with false representation of a social security number, in violation of 42 U.S.C. § 408(a)(7)(B), and aiding and abetting the same, in violation of 18 U.S.C. § 2; aggravated identity theft, in violation of 18 U.S.C. § 1028A, and aiding and

abetting the same, in violation of 18 U.S.C. § 2; and wire fraud, in violation of 18 U.S.C. § 1343. In addition, the affidavit supported an application for a search warrant for RIVERA's residence at 15 Brockton Avenue, Haverhill, Massachusetts. *See* 20-MJ-6557-MPK and 20-MJ-6560-MPK. A copy of Special Agent Taber's affidavit is attached to this affidavit as Exhibit 1 and incorporated by reference as though fully set forth herein. On September 9, 2020, this Court found probable cause and granted the applications for arrest and search warrants.

8. On September 10, 2020, DBFTF agents and officers executed federal arrest and search warrants at 15 Brockton Ave in Haverhill, MA. Based on the investigation to date, and the nature of the ongoing offenses, agents expected to uncover numerous fraudulent documents, stolen profiles, personal identifying information ("PII") and financial information related to stolen identities at RIVERA's residence.

9. As a result of the search, agents did discover these types of documents and information, including approximately twenty-nine fraudulent driver's licenses, and many of their accompanying social security cards and debit/credit cards. The majority of the fraudulent driver's licenses contained biographical information for different identities, yet contained photographs of the same nine individuals. Two of the fraudulent driver's licenses depicted [redacted].[1] The fraudulent licenses [redacted] were discovered hidden within a

[1] [redacted].

[2] The identity of victim F.P.R. is known to the government. In order, these initials represent the victim's first name, paternal last name and maternal last name.

[3] The identity of victim C.J.R. is known to the government. In order, these initials represent the victim's first name, middle name and last name.

hairbrush in the Infiniti SUV in the driveway. Also discovered hidden within a hairbrush in the Infiniti SUV was a social security card with social security number ending [redacted], Bank of America credit card and Bank of America debit card, all in the name of [redacted], which is a stolen identity used by [redacted] and is more fully discussed throughout this affidavit.

10. During the search, DBFTF members also located several money service business ("MSB") receipts for payments sent from targets of the investigation to suspected co-conspirators in the Dominican Republic in the kitchen of RIVERA's residence, including:

a. Three receipts were discovered in the name of [redacted], one of which listed an address of [redacted], which was the same address listed on the fraudulent [redacted] driver's license that depicted [redacted] One of the receipts indicated that on September 9, 2020, at approximately 1:24 pm, an individual purporting to be [redacted] transferred $970.00 from a MSB in Lawrence, MA to a male in the Dominican Republic, PERSON ONE.[4] The second receipt indicated that on September 9, 2020, at approximately 1:39 pm, an individual purporting to be [redacted] transferred $970.00 from a MSB in Lawrence, MA to an individual in the Dominican Republic. The third receipt in the [redacted] identity indicated that on September 9, 2020, at approximately 1:50 pm, an individual purporting to be [redacted] transferred $970.00 from a MSB in Lawrence, MA to an individual in the Dominican Republic. (All three transactions happened within 26 minutes and took place within

[4] The identity of this individual is known to law enforcement but withheld here because he is an uncharged co-conspirator.

approximately 0.3 miles of one another).[5]

b. Other receipts seized during the warrant documented that PERSON ONE received similar wire transfers from other targets of this investigation. For example, on September 3, 2020, someone using the name K.N.[6] transferred $970.00 to PERSON ONE. Also located within a hairbrush in the Infiniti SUV in the driveway, was a Georgia driver's license in the name of K.N. The license depicted Neida LOPEZ. LOPEZ was arrested, as part of this investigation, on September 10, 2020, and indicted on charges of conspiracy to commit wire fraud and aggravated identity theft on September 29, 2020, in *United States v. Neida Lopez,* 20-CR-40035.

c. One receipt listed [redacted] as the sender and listed [redacted] New Jersey Ave Apt. [redacted], Delanco 08075 as the sender's address. This is substantially the same address listed on the fraudulent [redacted] New Jersey driver's license that depicted [redacted] and was discovered during the search of RIVERA's residence. This receipt also documented the transfer of $970 to a recipient in the Dominican Republic. This transaction was made from the same store, on the same day, and within 7 minutes of the above transfer made by LOPEZ in the K.N. identity. Agents believe LOPEZ, using the K.N. identity, and [redacted] using the [redacted] and [redacted]

[5] Similarly, as described in the Criminal Complaints against Darwyn JOSEPH and Ramon CRUZ, additional MSB receipts were found inside RIVERA's residence indicating that both JOSEPH and CRUZ sent multiple wire transfers in the amount of $970 from MSBs in Lawrence, Massachusetts, to individuals in the Dominican Republic on September 9, 2020, under the direction of RIVERA and in furtherance of the conspiracy. *United States v. Ramon Cruz*, 20-mj-06782-MPK, Dkt. No. 4 ¶ 10; *United States v. Darwyn Joseph*, 20-mj-06781-MPK, Dkt. No. 4 ¶ 10.

[6] The identity of victim K.N. is known to the government. In order, these initials represent the victim's first name and last name.

identities, made these wire transfers to the Dominican Republic under the direction of RIVERA, in furtherance of the conspiracy further described below.

11. Agents also seized seven Chime[7] Debit/Visa cards during the search of RIVERA's residence. The Chime Cards were discovered in two places: (1) a red Nike bag in the kitchen, and (2) on the kitchen table. In addition to the physical Chime cards, an iPhone cell phone belonging to RIVERA was seized and subsequently searched pursuant to the warrant. Within the phone, agents located the identifiers for approximately 27 additional Chime accounts. RIVERA's phone also contained details of Chime accounts including, but not limited to the account holder's name, address, date of birth, social security number, account number, routing number, password and pin. The notes also listed which external bank accounts were linked to the Chime accounts as well as the addresses the Chime cards were ultimately mailed to, which is discussed further in paragraphs 26-41.

12. Additionally, RIVERA's cell phone contained numerous WhatsApp messages with Edwin ACEVEDO regarding the delivery, receipt, and activation of these Chime cards as well as the successful laundering of stolen SBA loan funds through purchasing and re-selling Apple iPhones using the Chime cards. Based on the investigation thus far, agents believe Edwin ACEVEDO, Ricardo ACEVEDO and Alvin RIVERA are siblings or half-siblings; both Ricardo ACEVEDO and RIVERA were charged in the original conspiracy, *United States v. Rivera et al.*, 20-cr-10228-PBS.[8]

[7] According to its web site, Chime is a financial technology company. It connects users to bank services provided by The Bancorp Bank or Stride Bank, N.A.

[8] For clarity, all references to "ACEVEDO" in this Affidavit refer to Edwin ACEVEDO. Ricardo ACEVEDO will be referred to only by his full name.

13. [redacted]

14. [redacted]

15. [redacted]

[9] [redacted]

[redacted]

[redacted]

16. [redacted]

[redacted]

[redacted]

17. [redacted]

18. [redacted]

[redacted]

10 [redacted]

11 [redacted]

[redacted]

19. [redacted]

20. [redacted]

21. [redacted]

[redacted]

22. [redacted]

23. [redacted]

24. [redacted]

ACEVEDO's Coordination of the Receipt and Activation of Chime Cards, and Laundering of Funds From Those Accounts, in Furtherance of the Conspiracy

25. As mentioned throughout this affidavit, an iPhone cell phone belonging to RIVERA was seized at his residence on September 10, 2020, and subsequently searched. Within this phone, agents discovered a WhatsApp chat with "$ ÇØRØNÃÛØ $" at 978-387-9728 that was initiated on June 19, 2020. Based on a photograph that was sent from $ ÇØRØNÃÛØ $ to RIVERA on September 6, 2020 that read, "How u like my $3,000 dollar swimsuit, I payed $7.00" and depicted an individual wearing a wetsuit. The individual depicted in the photograph was looking downward, such that his braids could be seen; his body type and hair are consistent

with the appearance of ACEVEDO's.[12] Additionally, agents have listened to various jail calls between RIVERA and ACEVEDO and have become familiar with ACEVEDO's voice. Within RIVERA's cellphone, user $ ÇØRØNÃÛØ $ sent numerous voice notes to RIVERA and I have determined that the voice recorded by the user of the $ ÇØRØNÃÛØ $ phone is the same voice of ACEVEDO in RIVERA's jail calls. Furthermore, a search of JOSEPH's cellphone conducted pursuant to federal warrant 21-MJ-6001-MPK, revealed that the phone number 978-387-9728 was saved in JOSEPH's phone as "Troubs." This investigation has revealed ACEVEDO's nickname to be "Trouble." Based on these facts, among additional information learned throughout this investigation, I have concluded the user of the contact saved as $ ÇØRØNÃÛØ $ in RIVERA's phone is ACEVEDO.

26. On August 22, 2020, at approximately 11:42 a.m., RIVERA sent the following WhatsApp message to $ ÇØRØNÃÛØ $:

"List of Chime Cards

K.J.N.[13]
[redacted]
LAWRENCE MA 01843
(CHIME) TITI 08/20th.

C.M.
[redacted]
DERRY NH 03038
(CHIME) CHAPI 08/21st.

B.K.M.
[redacted]
HAVERHILL MA 01830
(CHIME) MOM 08/24th.

[12] This comparison is based on ACEVEDO's photograph on file with the Massachusetts RMV as well as observations of ACEVEDO agents made on surveillance.
[13] The identity of victim K.J.N. as well as the subsequent eight identities listed in the above message sent to ACEVEDO are known to the government. In order, these initials represent either the victim's first, middle and last name or the victim's first and last name.

T.J.B.
[redacted]
LAWRENCE MA 01843
(CHIME) TITI 08/25th.

R.A.O.
[redacted]
MANCHESTER NH 03102
(CHIME) GLEY 08/26th.

D.P.C
[redacted]
NASHUA NH 03064
(CHIME) EVA MOM 08/27th.

H.L.F.
[redacted] S BROADWAY
LAWRENCE MA 01843
(CHIME) BLAKY

C.H.C.
[redacted] PERRY AVE [redacted]
METHUEN MA 01844
(CHIME) PÃŁMÅ

M.L.H.
[redacted]
MANCHESTER NH 03102
(CHIME) EVA BRO"

27. Based on information learned during this investigation, as well as my training and experience, I know the above message pertains to the delivery details of the Chime Cards that contained fraudulent SBA EIDL funds. The listed name signifies the Chime cardholder's name, followed by the address the cards were to be sent to, followed by the significance of the address (who resides there), followed by the expected delivery date. For example, the B.K.M. card was to be mailed to and received by "MOM" aka LOPEZ, at [redacted] in Haverhill, by August 24, 2020. As a second example, the D.P.C. card was to be mailed to and received by "EVA MOM" which is ACEVEDO's girlfriend Eva T[redacted]'s mother at [redacted]

[redacted] in Nashua by August 27, 2020. Additionally, the H.L.F. and C.H.C. Chime cards, related to "BLAKY" and "PALMA" refer to the cards received by CRUZ and JOSEPH respectively.

28. On August 25, 2020, at approximately 7:44 p.m., RIVERA messaged $ ÇØRØNÃÛØ $ and stated, "All the chimes are updated with new addresses n the replacement cards are getting mailed out." RIVERA then messaged, "So that's out the way finally now all we need to do is stay on top of the addresses the chime cards getting mailed out to." ACEVEDO then responded via the $ ÇØRØNÃÛØ $ device with a voice note stating, "Yea, nothing got to um my girl's house[14] and nothin got to Gley's house[15] yet. I checked them both."

29. On August 26, 2020, starting at approximately 11:45 am, ACEVEDO sent RIVERA a series of four photographs depicting Apple iPhone boxes, which detailed the serial numbers and other phone information. The first photograph depicted phone details of an iPhone 11 Pro Max with serial number FCHCJ38FN70K; the second, an iPhone 11 Pro Max with serial number FCHCJ43ZN70K; the third, an iPhone 11 Pro Max with serial number F2LCG1QJN70J; and the fourth, an iPhone 11 Pro Max with serial number F2LCF0J8N70J. Minutes later, RIVERA sent ACEVEDO an address of a CVS located in Methuen, MA to which ACEVEDO responded with a voice note stating, "If you want I can see that [racial slur] right now before I head up to Boston for the phones or I can see him on my way back down, you got to let me know right now." ACEVEDO later said via voice note, "So imma give him the whole 4 and then

[14] Based on my work in this investigation, I believe the reference to "my girl's house" to be a reference to ACEVEDO's girlfriend E[redacted] T[redacted]'s mother's home, at which the D.P.C. card was expected to arrive by August 24. *See* ¶ 26.

[15] Based on my work in this investigation, I believe the reference to "G[redacted]'s house" to be a reference to the house of G[redacted] A[redacted], a relative of ACEVEDO's, at which the R.A.O. card was expected to arrive by August 26. *See* ¶ 26.

just hold the other two for moms[16] so we can give them [inaudible] Puma." RIVERA responded, "Basicly today u keep the pay for two n I keep the pay for two." At approximately 12:22 pm, ACEVEDO messaged RIVERA, "Already seen em."

30. Transaction details and surveillance footage received from Apple show the above four iPhones were purchased from Apple stores in New Hampshire on August 26, 2020 between approximately 11:05 a.m. and 11:07 a.m., by JOSEPH and CRUZ using Chime Debit Card xxxx-xxxx-xxxx-1381 in the name of T.B. and Chime card xxxx-xxxx-xxxx-6306 in the name of B.M.[17]

31. Based on my familiarity with this investigation, as well as my training and experience, I believe ACEVEDO coordinated with CRUZ and JOSEPH to use the fraudulent Chime cards to purchase cell phones at a mall in New Hampshire. ACEVEDO then provided RIVERA with the make/model/gigabytes of the phones so that RIVERA could relay the information to an iPhone buyer in Massachusetts. RIVERA then provided ACEVEDO with an address in Methuen where ACEVEDO could meet the individual to physically transfer the phones for cash. ACEVEDO then messaged RIVERA stating, "Already seen em," which I believe to mean ACEVEDO had completed the transaction with the phone buyer.

32. Transaction details received from Apple for the above iPhones also showed all four phones were associated with phone numbers in Colombia approximately 30-60 days after they were originally purchased in New Hampshire. This leads me to further believe ACEVEDO was successful in meeting with and transferring the phones to the phone buyer as I have learned it is common for iPhone buyers to resell cellphones to other areas of the world for profit.

[16] As described elsewhere in this affidavit, "Mom" is an alias for LOPEZ.
[17] Both the -1381 T.B. and -6306 B.M. Chime cards were seized during the search warrant conducted at RIVERA's residence in September 2020. Additionally, both identities are detailed in RIVERA's note to ACEVEDO in paragraph 26, however without the middle initial.

33. On August 27, 2020, at approximately 10:58 am, the following WhatsApp conversation took place between RIVERA and ACEVEDO:

ACEVEDO (Audio)	Hey yo, fuckin um, Blaky[18] got the Chime card today
ACEVEDO (Audio)	Remember the one we sent to his house? He just got it.
RIVERA	Damn. That was fast.
ACEVEDO	H.F.
RIVERA	So hit Palma[19] up he might have got his also
ACEVEDO (Audio)	He's going to check when he goes home. He's in the gym right now

34. On August 27, 2020, at approximately 11:14 am, ACEVEDO sent RIVERA WhatsApp messages containing photographs of the front and back of the H.F. Chime Card ending in -2359. Within several minutes, RIVERA informed ACEVEDO that the card had been activated.

35. Based on my knowledge of this investigation, I know that "Blaky" is Darwyn JOSEPH and that JOSEPH lived at [redacted] S Broadway Lawrence, MA. I also know, based on transaction details provided by Chime Financial, that the Chime card in the name of H.F. was mailed to [redacted] S Broadway Lawrence, MA in August 2020 and, based on RIVERA's cell phone notes, had been expected to arrive on September 1, 2020. The above conversation demonstrates that ACEVEDO was involved in coordinating the receipt of the H.F. Chime card by JOSEPH in Lawrence, Massachusetts. Apple transaction details demonstrate that the H.F. Chime card ending in -2359 was used to purchase some of these iPhones at a mall in New Hampshire at approximately 2:05 pm. At approximately 3:00 pm, ACEVEDO began messaging RIVERA a series of photographs of iPhone serial numbers. Immediately after sending the photographs to RIVERA, ACEVEDO messaged, "Hit em up," which I interpret as ACEVEDO's telling

[18] This investigation has revealed that "Blaky" is a nickname for Darwyn JOSEPH.
[19] This investigation has revealed that "Palma" is a nickname for Ramon CRUZ.

RIVERA to contact the iPhone buyer so that ACEVEDO could again transfer newly purchased iPhones to the buyer to complete the laundering of the funds.

36. On August 31, at approximately 1:51 pm, RIVERA messaged ACEVEDO and stated, "Yo he can meet u at CVS in ten minutes." At approximately 2:02 pm, ACEVEDO replied, "Here. Where he at?" RIVERA then stated, "He should be there soon if isn't already." After reinitiating the conversation and discussing another topic, ACEVEDO informed RIVERA that he "already dropped that off" and that they "have 48 over there." In response, RIVERA stated, "Tato we getting there in due time we need to get to the millions that's always my goal."

37. Based on my training and experience, as well as my familiarity with this investigation, I believe ACEVEDO successfully transferred the iPhones purchased with fraudulent proceeds to the iPhone buyer in Massachusetts and received cash in return. I believe ACEVEDO then transported the money to a location known by both ACEVEDO and RIVERA and informed RIVERA that they had accumulated $48,000 in proceeds at that time.

38. On August 31, 2020, starting at approximately 9:14 pm, RIVERA messaged ACEVEDO and asked, "How many u have over there," to which ACEVEDO responded, "3 with Palmas. RIVERA then responded, "N with G[redacted]'s it's 4." ACEVEDO subsequently messaged RIVERA two photographs depicting the front and back of the C.C. Chime Card ending in -3769. Seconds later, ACEVEDO messaged RIVERA a photograph of what appears to be the letter the Chime card was mailed with, which showed the name C.C. followed by [redacted] Perry Ave. Apt.1 Methuen, MA. Approximately twenty minutes later, RIVERA informed ACEVEDO that the card had been activated. Apple transactions showed the C.C. Chime card ending in -3769 was first used at an Apple store at the Pheasant Lane mall in Nashua, NH on September 1, 2020. Furthermore, Apple surveillance footage showed ACEVEDO himself,

making purchases with the C.C. Chime card ending in -3769 at the Pheasant Lane mall on September 2, 2020.

39. Based on my knowledge of this investigation, I know that "Palma" is Ramon CRUZ and that CRUZ was associated with [redacted] Perry Ave. Apt.1 Methuen, MA. I also know, based on transaction details provided by Chime Financial, that the Chime card ending in -3769 in the name of C.C. was mailed to [redacted] Perry Ave. Apt.1 Methuen, MA, and, based on Rivera's phone notes, that it was expected to arrive by September 1. The above conversation suggested that ACEVEDO took part in receiving the C.C. Chime card in Methuen, Massachusetts. Additionally, by cross-referencing the time stamp on Apple store surveillance footage with the listed transactions provided by Apple, it was apparent ACEVEDO used various Chime cards containing funds from fraudulently-obtained SBA EIDL loans, including the C.C. Chime card ending in -3769, to purchase iPhone 11 Pro Max cellphones.

40. On September 1, 2020, WhatsApp messages between ACEVEDO and RIVERA, suggest that ACEVEDO had received yet another Chime card on behalf of RIVERA. At approximately 2:33 pm, ACEVEDO messaged photographs of the account details and back of a R.O. Chime card ending in -0916. Chime Financial subpoena results indicated the R.O. card was mailed to [redacted] Manchester, NH, which is associated with ACEVEDO's relative "G[redacted] A[redacted]." A note in RIVERA's phone also indicated that "Gley" was expected to receive a Chime card in the R.A.O. identity on August 26. Less than two hours after ACEVEDO sent the images of the front and back of the card to RIVERA, Apple transaction details show the R.O. Chime card ending in -0916 was used at an Apple store at the Pheasant Lane mall in Nashua for the purchase of two iPhone 11 Pro Max cellphones. Apple

surveillance footage depicts ACEVEDO himself using the R.O. Chime card ending in -0916 to make an Apple purchase at the Pheasant Lane mall on September 2, 2020.

41. During the September 10, 2020 search of RIVERA's residence at 15 Brockton Ave, agents located and seized Chime Debit Card xxxx-xxxx-xxxx-0916 in the name of R.O. Agents subsequently learned that $25,100 in funds from an SBA EIDL had been deposited into the account associated with that card on or about August 3, 2020. Chime Financial records for this account show that the account contained a linked Automatic Clearing House ("ACH") account, which was Bank of America account number xxxx-xxxx-4902 – the account that, as described in paragraph 17, GARCIA had opened in the F.P.R. identity.

[redacted]

42. [redacted]

43. [redacted]

44. [redacted]

45. [redacted]

[20] [redacted]

46. [redacted]

Summary of Defendants' Involvement with Economic Injury Disaster Loan and Wire Fraud Conspiracy

47. Based on the investigation to date, described further below, as well as my training and experience, I believe probable cause exists to believe that ACEVEDO and [redacted] assisted RIVERA in a conspiracy to steal the identities of actual United States citizens, use their personal information to apply for EIDLs from the SBA, to receive at Massachusetts residences Chime cards linked to bank accounts containing the fraudulently-obtained EIDL funds, and to launder the stolen funds by transferring cellphones for cash and using interstate wires in furtherance of the conspiracy. I form this opinion based on my training and experience and based upon a number of factors, including [redacted] involvement in opening a fraudulent bank account which was linked to a stolen EIDL, ACEVEDO's receiving in the mail Chime cards connected to bank accounts containing stolen EIDL funds, their laundering of funds from the Chime accounts by purchasing bulk iPhones for re-sale, their sending profits or facilitating the sending of profits of the conspiracy to co-conspirators in the Dominican Republic, and many of their communications with RIVERA.

48. As discussed in detail above, [redacted] opened an account with Bank of America on or about July 21, 2020. Bank records show minimal activity occurred within the checking account thereafter, aside from mainly ATM withdrawals and transactions related to the funding

or verification of other accounts at financial institutions. Based on my familiarity with the scheme, it is my opinion that [redacted] opened a checking account with Bank of America (1) to apply for a credit card with Bank of America and purchase merchandise on credit that would never be paid back; and (2) so that RIVERA and others could link the accounts to other fraudulent accounts for the purpose of accepting money transfers, such as from Chime/Stride Bank accounts in the name of R.O.

49. In total, agents identified approximately $452,204 in SBA funds that had been sent to Chime accounts associated with Chime debit cards that were seized from 15 Brockton Ave and/or whose account details were stored in RIVERA's cellphone. Chime records indicated approximately $250,000 of this money was used to purchase iPhones at Apple stores in Massachusetts and New Hampshire, which I learned were then re-sold for cash, resulting in the laundering of thousands of dollars related to SBA EIDLs – a process that both ACEVEDO and [redacted] were involved in, in furtherance of the conspiracy. On December 16, 2020, approximately $200,000 of the fraudulent SBA loan funds were recovered and seized by HSI pursuant to 20-6763-MPK through 20-6771-MPK.

50. Agents contacted Apple for transaction details related to all Chime accounts referenced throughout this affidavit. Agents received detailed records of hundreds of transactions that took place between August 14, 2020 and September 9, 2020. The product description of every transaction was an iPhone 11 Pro Max 256 gigabyte phone with an original price of $1,249. Apple results also revealed several different Chime cards were used to make the purchases, often within minutes of one another, and from the same store. Additionally, Apple footage depicted ACEVEDO, LOPEZ, CRUZ, JOSEPH and others using the Chime cards to purchase the iPhones. Moreover, the photographs of iPhone serial numbers sent by [redacted] to

RIVERA on September 2, 2020 demonstrate that [redacted] was also involved in the laundering of funds from the Chime accounts through Apple stores.

51. I understand, based on this investigation, as well as my training and experience, that debit card transactions generally involve (1) the presentation of a debit card at a point of sale, (2) the "swiping" or reading of the debit card at the point of sale, and (3) the transmission of data about the transaction, via an internet connection or telephone line (i.e., through interstate wires), to the relevant bank or processor in order to confirm that the bank account with which the debit card is associated has sufficient funds for the transaction, and to commence the exchange of funds and effectuate the sale. Chime Financial/ Stride Bank utilizes a payment processor by the name of Galileo Technologies, which utilizes servers in Illinois, California, New Jersey, and Utah to process debit card transactions. The bulk of the Chime card purchases made in furtherance of this conspiracy took place in Massachusetts and New Hampshire. Accordingly, the Chime debit card transactions originating in Massachusetts and New Hampshire all involved interstate wires.

52. Moreover, in furtherance of the conspiracy, [redacted] was involved in sending a share of the profits of the conspiracy to co-conspirators in the Dominican Republic through money transfers at MSBs in Lawrence, Massachusetts. I understand, based on this investigation, as well as my training and experience, that money transfers through money service businesses are effectuated over the internet. A money transfer from a MSB in Massachusetts to a recipient in the Dominican Republic involves interstate wires.

Probable Cause That Evidence, Fruits, and Instrumentalities of the Target Offense Will Be Found at the Target Location

53. ACEVEDO's girlfriend Eva T[redacted] (who has been identified as participating in this fraudulent scheme), is currently receiving U.S. Department of Housing and Urban

Development (HUD) benefits at the Target Location. Records show the date the unit last passed inspection was November 11, 2020 with a listed address of "[redacted] Trillium Way, Acton, MA[21]" and stated her mailing address was the same as the unit address.

54. On July 20, 2021, Acton police officers encountered ACEVEDO and T[redacted] in the area of 1300 Avalon Drive in Acton, MA for a report of a green motorcycle riding without a license plate. Upon questioning ACEVEDO and T[redacted], they each reported their residence as [redacted] Trillium Cir. Acton, MA to police officers.

55. On July 22, 2021, at approximately 10:04 am, while conducting physical surveillance of [redacted] Trillium Cir. Acton, MA, DBFTF agents observed ACEVEDO exit the Target Residence via the garage door and enter a green Mazda pickup truck. The truck was registered to G[redacted] A[redacted] of [redacted] Manchester, NH. Agents soon thereafter lost sight of ACEVEDO but observed him drive back to the Target Residence in the Mazda several hours later.

56. On July 28, 2021, at approximately 9:15 pm, DBFTF agents conducted a drive-by of the Target Residence and observed ACEVEDO's green Mazda pickup truck parked across from the garage to [redacted] Trillium Cir.

57. On July 29, 2021, at approximately 6:15 am, DBFTF agents established surveillance of [redacted] Trillium Cir. Acton, MA and noticed ACEVEDO's green Mazda pickup truck appeared to be parked in the same parking space as agents observed the night prior. At approximately 10:12 am, DBFTF agents observed ACEVEDO exit the Target Residence via the garage door and subsequently enter the same green Mazda pickup truck and depart the area. At

[21] Based on open-source documents, it does not appear [redacted] Trillium Way, Acton, MA exists, and should actually read [redacted] Trillium Cir, Acton, MA

approximately 2:25 pm, agents observed ACEVEDO, driving the Mazda pickup truck, arrive at and enter the Target Residence. At approximately 2:38 pm, agents observed ACEVEDO exit the Target Residence and walk in the direction of the mailboxes with nothing in his hands. Moments later, ACEVEDO was observed carrying and perusing through what appeared to be mail. He then reentered the Target Residence.

58. On August 9, 2021, at approximately 10:35 pm, DBFTF agents conducted a drive-by of the Target Residence and observed ACEVEDO's green Mazda pickup truck parked across from [redacted] Trillium Cir.

59. On August 12, 2021, at approximately 6:20 am, DBFTF agents conducted a drive-by of the Target Residence and observed ACEVEDO's green Mazda pickup truck parked across from [redacted] Trillium Cir.

60. I know, based on my training and experience, that:

a. Individuals often keep identification documents and financial records and other evidence of identity for long periods – sometimes years – and tend to retain such documents even when they depart a given residence. Such documents include driver's licenses, social security cards, bank cards, credit cards, bank records, and credit card statements.

b. Individuals often keep identification documents and financial records in their residence, in part to ensure the security of these documents and in part to allow for access to these documents when needed.

c. In addition, it is common for those who use other persons' identities without authorization to maintain fraudulently obtained identification documents in secure locations within their residence to conceal them from

law enforcement authorities;

d. It is common for individuals who use fraudulently obtained identification documents to retain those documents for substantial periods of time so that they can continue to use the fraudulently obtained identities;

e. Individuals involved in making false identification documents often use computers, cell phones, printers, and similar equipment to create the false identification documents. This equipment is often stored in the individual's home. This equipment is expensive and durable, and can be stored and used for years; and

f. Based on my experience and training, I also know that individuals who make purchases of goods and services often retain their receipts and invoices in their residence.

61. I also know, based on my training and experience:

a. Individuals frequently use computer equipment to carry out, communicate about, and store records regarding their daily activities. These tasks are frequently accomplished through sending and receiving e-mail, instant messages, and other forms of phone or internet based messages; scheduling activities; keeping a calendar of activities; arranging travel; purchasing items; searching for information including information regarding travel and activities; arranging for travel, accessing personal accounts including banking information; paying for items; and creating, storing, and transferring images, videos, and other records of their movements and activities.

b. Individuals involved in criminal activity, to include the planning and execution of identity theft schemes, communicate with each other through the use of cellular telephones. Additionally, I am also aware that individuals involved in criminal activity, to include the planning and execution of identity theft schemes, communicate using social media networking sites like Facebook, Snapchat, WhatsApp, etc. which can be accessed through cellular telephones.

c. I know that many smartphones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

d. I am aware that individuals commonly store records of the type described in Attachment B in mobile phones, computer hardware, computer software, and storage media.

e. I know that data can often be recovered months or even years after it has been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

i. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when

users replace their electronic equipment, they can easily transfer the data from their old device to a new one.

ii. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a device, the data contained in the file often does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, the device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

iii. Wholly apart from user-generated files, electronic storage media often contains electronic evidence of how the device has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but users typically do not erase or delete this evidence because special software is typically required for that task.

iv. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are

overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

v. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

vi. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience,

information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and

the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

vii. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

viii. The process of identifying the exact files, blocks, registry entries,

logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

ix. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

62. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true

because of:

a. The volume of evidence — storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements — analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a “booby trap.”

Consequently, law enforcement agents may either copy the data at the premise to be searched or seize the computer equipment for subsequent processing elsewhere.

63. The premise may contain computer equipment whose use in the crimes or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premise during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

64. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied, or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Conclusion

65. Based on the foregoing, I submit there is probable cause to believe that Edwin ACEVEDO, between June 19, 2020 and August 18, 2021, having conspired with others known

and unknown to commit wire fraud, that is, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, which schemes involved the transmission by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, for the purpose of executing the scheme to defraud, to include, stolen identity information to Apple Inc., Bank of America, Chime Financial, Stride Bank, and Galileo Technologies, in violation of Title 18, United States Code, § 1343, all in violation of 18 U.S.C. § 1349.

66. [redacted]

67. Based on the forgoing, I also have probable cause to believe that evidence, fruits, and instrumentalities of the Target Offense, as described in Attachment B, are located in the premises described in Attachment A.

Signed under the pains and penalties of perjury this 18th day of August, 2021.

_____
Jacqleen M. Cunningham
Special Agent
Homeland Security Investigations

Subscribed and sworn to via telephone in accordance with Federal Rule of Criminal Procedure 4.1 this 18th day of August 2021.

_____
HONORABLE M. PAGE KELLEY
CHIEF UNITED STATES MAGISTRATE JUDGE
DISTRICT OF MASSACHUSETTS